

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

04/09/2014

SUBJECT:

Multiple Vulnerabilities in Google Chrome Could Allow Remote Code Execution

EXECUTIVE SUMMARY:

Multiple vulnerabilities have been discovered in Google Chrome that could result in remote code execution. Google Chrome is a web browser used to access the Internet. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the affected application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

At this time, there is no known proof-of-concept code available.

SYSTEM AFFECTED:

- Google Chrome Prior to 34.0.1847.116

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Fourteen vulnerabilities have been reported in Google Chrome. Details of the vulnerabilities are as follows:

- An authentication-bypass vulnerability exists in the V8. [CVE-2014-1717]
- An out-of-bounds vulnerability exists in the V8. [CVE-2014-1717]
- An integer-overflow vulnerability exists in the compositor. [CVE-2014-1718]
- An use-after-free vulnerability exists in the web workers. [CVE-2014-1719]
- An use-after-free vulnerability exists in the DOM. [CVE-2014-1720]
- A memory-corruption vulnerability exists in the V8. [CVE-2014-1721]
- An use-after-free vulnerability exists in the rendering. [CVE-2014-1722]
- A security vulnerability exists due to URI confusion with RTL characters. [CVE-2014-1723]
- An use-after-free vulnerability exists in the speech. [CVE-2014-1724]
- An authentication-bypass vulnerability exists with window property. [CVE-2014-1725]
- An unspecified local cross-origin policy security-bypass vulnerability. [CVE-2014-1726]
- An use-after-free vulnerability exists in the forms. [CVE-2014-1727]
- Multiple security vulnerabilities due to an unspecified error. [CVE-2014-1728]
- Multiple security vulnerabilities due to an unspecified error V8. [CVE-2014-1729]

Successful exploitation could result in an attacker gaining the same privileges as the affected application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

RECOMMENDATIONS:

The following actions should be taken:

- Update vulnerable Google Chrome products immediately after appropriate testing by following the steps outlined by Google.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

- Do not open email attachments or click on URLs from unknown or un-trusted sources.

REFERENCES:

Google:

<http://googlechromereleases.blogspot.com/2014/04/stable-channel-update.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1716>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1717>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1718>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1719>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1720>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1721>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1722>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1723>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1724>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1725>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1726>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1727>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1728>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1729>